Version 2.0 May 2020

China CITIC Bank
London Branch

Operational Risk Management Policy

中信银行
CHINA CITIC BANK
伦敦分行
LONDON BRANCH

Document History

Author	Chief Risk Officer	Status	Approved
Version	2.0	Date	May 2020
Approved by	Management Committee		
Approved Date	22/5/2020	Next Review Date	March 2021
Location	London		

Version	Owner	Approval	Date	Major changes
1.0	President	President	May 2018	PRA Regulatory Business Plan
1.1	CRO	MANCO	October 2018	As per ManCo approval Oct 2018
2.0	CRO	MANCO	May 2020	• No changes proposed

CONTENTS

1 Introduction

Operational risk may arise from various internal and external factors relating to people, process and systems.

This policy document sets out China CITIC Bank London Branch's ("CNCBLB's" and / or "the Branch's") overarching approach to Operational Risk Management.

2 Objectives

The purpose of this policy is to set out China CITIC Bank London Branch's ("CNCBLB" or the "Branch") approach to Operational Risk Management ("ORM").

Operational risk is identified as a separate and distinct category of risk similar to credit and market risk. The management of operational risk as a distinct risk category along with credit and market risks is a manifestation of the vital role played by operational risks in impacting the Branch's risk profile. Management of operational risk includes its identification, assessment, control / mitigation, monitoring and reporting.

This operational risk management framework forms part of CNCBLB's overall risk management framework. The high-level objectives of CNCBLB's ORM Policy are:

- To capture the operational risk management framework in place at CNCBLB and is designed to be commensurate with the scale, risk profile and risk appetite of the Branch;
- Support a risk culture and environment for the effective management of operational risk within CNCBLB;
- Set out the governance structure and roles for each of the three lines of defence in relation to operational risk management; and
- Support the embedding of the ORM into the day to day business of CNCBLB.

3 Document Ownership

The 'ownership chain' for this policy document is outlined below:

Document Owner	The Chief Risk Officer ("CRO") is responsible for the maintenance of this document and ensuring that it is reviewed annually, or more frequently as required.
Challenge	The Audit and Risk Committee ("ARCo") will review this document annually or more frequently as necessary. The ARCo will provide its recommendation to the Management Committee ("ManCo") for approval or otherwise.
Approval	Based on recommendations by ARCo, ManCo review and challenge the ORM Policy before approving it (or otherwise). This must happen following each review by ARCo.
Applicability	All members of staff, whether permanent (local hires and expatriate alike) or contractors must adhere with the provisions of this document and all policies associated therewith. Escalation of any matters arising in respect of this should be via the individual's Head of Department or directly to the CRO.

4 Overview of Operational Risk Management

4.1 Definition of Operational Risk

Operational Risk is defined as the risk of an economic loss, a disruption to business, an adverse impact on reputation or on client relationships or of legal action arising from inadequate or failed internal processes, people and systems. The definition is "causal-based", providing a breakdown of operational risk into four categories based on its sources:

- People;
- Processes;
- Systems; and/or
- External factors

4.2 Sources of Operational Risk

CNCBLB recognises that operational risk could arise in a number of different from the underlying business activities. The categories defined by this policy are based on the BASEL operational risk categories which are summarised as follows:

OPERATIONAL RISK	BASEL EVENT TYPE	BASEL EVENT TYPE	BASEL EVENT TYPE
	LEVEL 1	LEVEL 2	LEVEL 3
PEOPLE RISK	**Internal Fraud**	. Unauthorised activity . Theft / fraud	. Transcat not reported . Transaction not approved . mismarking poistion . Extortion / embezzlement . Misappropriation / forgery . Malicious damage . impersonation/insider trading . Bribes /kick-backs
	External fraud	. Theft / fraud . System security	. Theft / robbery / forgery . Hacking damage . Theft of information
	Employment Practices and Workplace Safety	. Employee relations . Diversity / Discrimination	. Comensation / benefits . Organised lobour activity . All discrimination types
PROCESSESS RISK		. Safe Environment	. General liability (slips, falls…) . Health & Safety rules . Workers compensation
	Clients, Products & Business Practices	. Suitability, disclosure, fiduciary . Selection, sponsorship, exposure	. Fiduciary / expousre breach .Disclosure issues(KYC, Privacy) . Aggressive sales /Liability
		Improper business/ market practice	. Improper transactions . Market manipulation . Insider trading (firm) . Unlicensed activity . Product defects
	Execution, Delivery & Process Management	. Transaction capture / execution . Monitoring & reporting . Customer onboard / management . Vendor /suppliers	. Miscommunication /errors . Poor performance / failures . Data management / records . Failed mandatory reporting . Outsourcing / disputes
	Business disruption and system failures	Systems	. Hardware / software . Telecommunications
SYSTEMS RISK		Security	. Cyber attacks /malware . Virus protection
EXTERNAL RISK	**Damage to Physical Assets**	Disasters and other events	. Human (vandalism/terrorism) . Pandemics . Natural (weather/water…)

4.3 Operational Risk Appetite

CNCBLB has a very low tolerance for operational risk and strives to reduce operational risk, whenever it is cost beneficial or required by law and regulation, to a level which is acceptable. The Branch's operational risk appetite is outlined in its Risk Appetite Statement ("RAS") and presented in **Appendix A**, which is reviewed at least annually.

5 Operational Risk Governance, Roles and Responsibilities

This section sets out the roles and responsibilities of different committees and business areas in the context of Operational Risk Governance.

5.1 Role of ManCo

ManCo is responsible for:

- Setting the operational risk appetite as part of the overall risk appetite statement;
- Reviewing the recommendations of the ARCo and approving the operational risk management arrangements; and
- Reviewing reports of operational risk incidents, near misses and Key Risk Indicator ("KRI") threshold breaches
- Approving the Risk Matrix which contains the complete list of operational risks and their mitigants.
- Deliberating on training requirements, including in relation to operational risk.

5.2 Role of ARCo

ARCo is responsible for:

- Reviewing the risk appetite statement annually and suggesting any changes to the ManCo for challenge and approval;
- Reviewing the adequacy of the operational risk management arrangements and making recommendations to the ManCo for approval;
- Reviewing reports of operational risk incidents, near misses and Key Risk Indicator ("KRI") threshold breaches and escalating specific matters to HO if necessary; and
- Reviewing the suite of operational risk KRIs and calibration of KRIs at least bi-annually or as necessary.

5.3 Role of the First Line

In particular, the first line functions are responsible for the following (non-exhaustive list):

- Ensuring implementation of CNCBLB's operational risk management framework and corresponding policies and procedures;
- Identifying operational risks and liaising with the Risk Department to capture them in the Risk & Control Self-Assessments;
- Developing and reporting breach of KRI trigger thresholds to the ManCo and recommending mitigation action;
- Reporting operational risk incidents and near misses to the Risk Department;
- Implementation of corrective and preventative action plans as per agreed timelines;
- Participation in training programs;
- Implementation of Operational Risk controls including the preparation of procedural documentation to support implementation of relevant policies; and
- Putting in place the required insurance to support CNCBLB's operations.

5.4 Role of the Second Line

The Risk Department performs CNCBLB's second line of defence in relation to operational risk. Its responsibilities include but are not limited to the following areas:

- Designing the ORM framework;
- Drafting policies and defining policy standards to be adhered to by the first line;
- Maintaining, monitoring and reporting the incident /near miss events, overall risk matrix/register and root cause analysis;
- Maintaining, monitoring and reporting the departmental risk & control self-assessments;
- Oversight of the implementation of operational risk management arrangements by the first line;
- Reviewing and challenging the operational risk management tools and controls used by the first line;
- Defining and monitoring the KRIs against trigger thresholds;
- Providing KRI MI on a monthly basis to the Manco;
- Co-ordinating with the HO ORM Department for implementation of ORM framework at Bank wide level;
- Promoting a strong operational risk culture within CNCBLB and ensuring employees are aware of their responsibilities;
- Developing and delivering training; and

- Advising on the operational risk implications of future business plans and new products.

5.5 Role of the Third Line

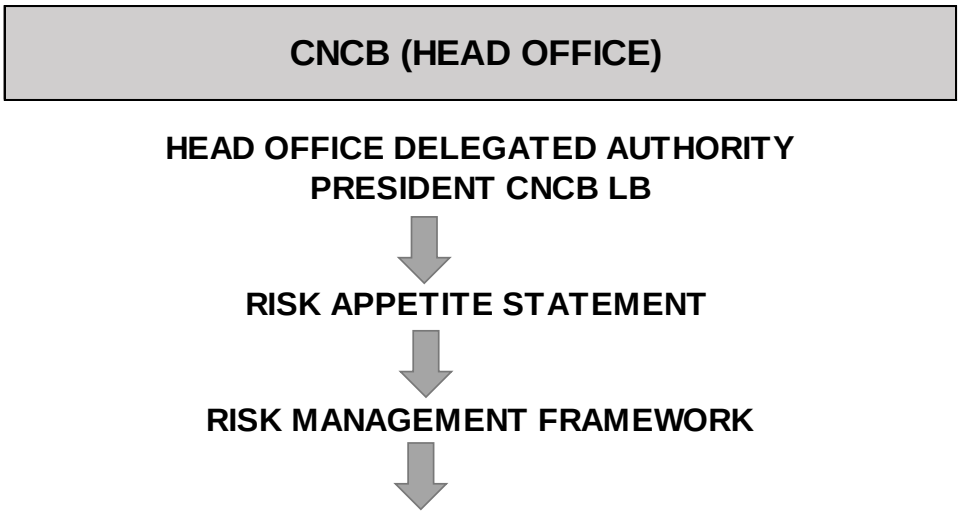
The role of the third line of defence is to provide assurance on the effectiveness of the ORM policy and its implementation as applicable to the first and second lines of defence. The third line will be provided by an external third-party Service Provider on an outsourced basis. Operational Risk Management is one of the specified areas that will be covered in the Internal Audit Plan.

The Internal Auditors will report to the President of CNCBLB.

6 Operational Risk Management Framework

6.1 Risk Management Framework

Operational Risk management forms and integral part of the overall risk framework, which is presented as follows:



RISK	PRIMARY RISK MANAGEMENT FRAMEWORK
CREDIT RISK	Credit Approval and Credit Risk Management Policy
MARKET RISK	Market Risk Management Policy
OPERATIONAL RISK	Operational Risk Management Policy Outsourcing Policy Business Continuity Management Framework New Products Approval Policy Conduct Risk Policy Framework
LIQUIDITY RISK	Liquidity Risk Management Policy

Risk department will manage operational risk that includes the policies identified above and using the following tools to identify, measure, manage and report operational risk:

- Incident/Near Miss register (See **Appendix B**)
- Risk & Control Self-Assessments (See **Appendix C**)
- Key Risk Indicators (See **Appendix D**)

The Branch is committed to identifying, assessing, monitoring, controlling, mitigating, and reporting operational risk through an operational risk management framework.

Each stage is discussed below.

6.2 Operational Risk Identification

Operational risk is inherent in all the Branch's activities and operations shall be identified on a pro-active basis including risks in outsourcing and on introduction of new products, systems, processes and any material changes therein.

Operational risk identification is the responsibility of First Line functions (the business and supporting functions). Operational risks will be identified through event reporting to Risk department through the 'Incident/Near miss' process that will be captured in the CNCBLB Risk Matrix, which captures the full universe of risks arising from the business conducted by CNCBLB.

Each year the Risk Matrix is updated through a bottom-up approach whereby individual departments 'Risk & Control Self-Assessments whereby the Business heads review/update risks relevant to their business areas. Given that operational risks can arise anywhere within the business, all department heads should review/update operational risks as part of their annual review.

Department heads will work with Risk department to ensure a thorough review of existing and emerging risks and will not assume that certain operational risks will be covered by other department heads.

The Chief Risk Officer will also be responsible for identifying existing and emerging operational risks through this bottom-up approach and will have a view of operational risks identified/reviewed/updated by all department heads to ensure no operational risks are omitted from the Risk Matrix.

6.3 Operational Risk Assessment

Each Operational risk identified will assessed using the template in Appendix B which will include:

- Causal area
- Impacted area
- Root cause
- Loss (actual or potential)
- Corrective action
- Preventative action

In addition to identifying the operational risks it is subject to, CNCBLB periodically assesses its vulnerability to these risks.

Operational risks are assessed in accordance with CNCBLB's Risk Scoring Methodology (See **Appendix E**) which assigns an overall risk rating for each operational risk identified based on the impact and probability. The assessment is considered both before ('gross') and after mitigating controls ('net') have been implemented and the results contained within the Risk Matrix.

6.4 Operational Risk Control and Mitigation

CNCBLB periodically reviews risk control and mitigation strategies to ensure these remain effective and relevant, in light of its overall risk appetite and profile.

For all material operational risks that have been identified and rated as Medium or High, CNCBLB shall decide whether to use appropriate procedures to control and / or mitigate the risks or bear the risks. For those risks that cannot be controlled, CNCBLB shall decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

The decision to adopt an appropriate risk treatment is based on balancing cost and risk while always ensuring regulatory compliance. This decision is made by ManCo based on recommendation from the ARCo through the periodic risk assessment as captured in the Risk Matrix.

6.5 Operational Risk Analysis and Monitoring

Analysis and continuous monitoring of operational risk is vital for the effective management of operational risk.

Monitoring of operational risk exposures is necessary to protect the Branch and implement appropriate mitigation. To this end, CNCBLB will developed a Key Risk Indicators to monitor the level of operational risk CNCBLB is exposed to in various areas (See Appendix D).

The Risk Department will be responsible for the monitoring of these KRIs and providing MI to the ManCo on a monthly basis. The suite of KRIs and calibration of KRIs will be reviewed at least bi-annually or as necessary by the ARCo.

In addition, CNCBLB shall also monitor and analyse internal and external developments which affect CNCBLB's operational risk profile such as business strategy, introduction of new products, process, systems or decisions with regards to key outsourcing, changes in the regulatory, business, economic, political and social environment.

6.6 Operational Risk Reporting

The Risk Department will provide monthly MI to the ManCo on operational risk covering:

- Operational Losses (Basel categories, causal area, impact area, trend analysis)
- Operational Events (High, Medium, Low & causal/impacted areas)
- Key Risk Indicators (Status/trend)
- Key Risk Indicator breaches (explanation)Controls and Mitigation

For all material operational risks that have been identified, CNCBLB shall decide the appropriate risk treatment such as acceptance, reduction, avoidance or transfer.

An appropriate risk treatment depends upon various factors such as:

- Nature of the risk;
- Risk appetite;
- Business strategy;
- Available risk measures;
- Cost / Benefit; and
- Regulatory requirements.

6.7 Systems and controls

CNCBLB has a robust set of systems and controls in place to mitigate operational risk. Internal controls are embedded in a bank's day-to-day business at all levels.

CNCBLB's systems and controls that mitigate operational risk include:

- The CRO has the ultimate responsibility for putting in place effective systems and controls for mitigating operational risk;
- Appropriate segregation of duties such that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest are to be identified, minimized, and subjected to careful independent monitoring and review;
- The Organogram is updated regularly with clear reporting lines;
- Job descriptions are provided to all staff members;
- Performance appraisal process that evaluate each role against the job descriptions;
- Periodic investment in IT infrastructure including various hardware/software tools that support the operations;
- Four eyes principles in operations;
- Clearly established authorities and/or processes for approval;
- Close monitoring of adherence to assigned risk thresholds or limits;
- Safeguards for access to, and use of, CNCBLB assets and records;
- Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
- Regular verification and reconciliation of transactions and accounts;
- A robust technology infrastructure is in place that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management;
- Effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel;
- Adequate training to all the staff members; and
- Adequate MI for the management for decision making.

6.8 Policies and procedures

CNCBLB's operational risk framework is comprised of a range of policies and procedures to mitigate operational risk. Policies that impact Operational risk directly are summarised below:

Policy/Procedure Title		Policy Owner
Risk Appetite Statement	Defines the Branches business activities, target market and risk appetite	Chief Risk Officer
Governance & Risk Management Framework	Sets out the regulatory environment, overarching risk framework and committee structures	Chief Risk Officer
Risk Matrix	Consolidates all the identified risks within the Branch which are assessed for inherent and residual risks.	Chief Risk Officer
Outsourcing Policy		Chief Risk Officer
Business Continuity Management Framework		Chief Risk Officer
New Products Policy	Defines the process in which new products and changes to existing products can be approved	Chief Risk Officer
Conduct Risk Policy		Chief Risk Officer

6.9 Training

To support this and ensure that staffs are equipped with the necessary knowledge to undertake their roles effectively staffs will be required to undertake periodic training as well as complete an induction programme upon joining the Branch. The Operational risk training will cover a minimum of:

- Overview of Operational Risk (Basel risk categories and principles of sound management of operational risk)
- Operational risk drivers (Top 10 risks, risk matrix, risk framework and risk appetite)
- Operational event reporting (Incident/near miss register and root cause analysis)
- Risk & Control Self-Assessments (risk identification and assessment)
- Key Risk Indicators (strategic, tactical and dynamic KRI's)
- New Product Policy (Business case, assessment and sign-off)

- Outsourcing Risk (Regulatory requirements, process and assessment)
- Business Continuity Framework (HO recovery and London Branch)
- Conduct Risk (High level overview, Policies, conduct rules and CNCB culture)

CNCBLB maintains a record of all training completed (title of training and date completed) and where applicable, certification that such training has been received and absorbed by current staff members together with an archive which contains the training records of all leavers (regardless of the reason for leaving) for a minimum period of five years post departure.

6.10 Compliance monitoring program

CNCBLB operates a compliance monitoring program to ensure it remains compliant with applicable regulations at all times. This reduces the likelihood of CNCBLB incurring loss through legal or regulatory breaches.

6.11 Insurance

Insurance policies, particularly those with prompt and certain pay-out features, can be used to mitigate the risk of “low frequency, high severity” losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

Before taking out insurance against the risk must first have been determined as suitably specific and with definable as well as predicable features allowing adequate cover to be agreed with an insurer. This assessment will be made by the ARCo with ManCo, based on the CRO’s recommendation to seek insurance cover as a risk mitigant.

For the cost of insurance to be deemed acceptable, the cost must be at a comparable level to the benefits to be obtained in case the risk covered materialises. A decision to retain either all or a residual risk position may be deemed appropriate where cost benefit-analysis shows there to be an adequate economic return/limited probability of risk crystallisation to make up for this.

7 Review and Update of Policy

The Operational Risk Policy shall be reviewed by the Risk at least annually or as directed by the ManCo, to reflect changes in the profile of risks or business activities, organisational or authority structures or new regulations relevant to CNCB LB management of market risk.

8 Appendix A – Risk Appetite

The Risk Appetite with respect to operational risk is as follows:

CNCBLB is a start-up operation and therefore has no historical data and may be subjected to higher people, processes and system risks in the initial stage of its strategic development. In order to quantify an acceptable risk appetite for operational risk exposure, a dynamic methodology will be monitored by risk department to manage the higher risk in the initial stages; this risk will reduce as the people, process and systems are strengthen over time, the following table refers:

	Year 1	Year 2	Year 3	Year 4	Year 5
Operating Income	$3,100,000	$5,600,000	$11,100,000	$17,300,000	$23,600,000
Tolerance Risk Appetite (bps)	1.25	0.85	0.50	0.25	0.25
Ops Risk Appetite	**$38,750**	**$47,600**	**$55,500**	**$43,250**	**$59,000**

9 Appendix B – Incident/Near Miss template & Log

The Incident/Near Miss register will be maintained by Risk Department. The register will cover the following:

Event	Risk Assessment
• Event number • Date of event • Date reported to Risk Department • Causal area • Impacted area • Event summary • Actual loss • Potential loss • Root Cause	• Risk Rating (High, Medium, Low) • Primary cause (People, Process, System) • Cause category (Basel category) • Remedial action (corrective action) • Preventative Action (control enhancement) • Event assigned to…. • Event status (open, work-in-progress, action plan agreed, closed) • Closure date

Risk Event Data Collection

CNCBLB shall establish a framework for identifying and recording risk events which shall include:

a) Operational risk events causing financial loss
b) Operational risk events having an indirect impact, such as:
    i. Reputation risk events
    ii. Regulatory breach
    iii. Health and safety incidents
    iv. Business disruption incidents

The business owners/first line of defence departments are responsible for reporting any operational risk events. Risk Department shall track risk events on an on-going basis to monitor changes in the level of threat to the business and to assist in considering the quality, design and implementation of its controls.

At the occurrence of a risk event, Risk Department shall ensure that all relevant loss data (if any) is collected and shall consider the collection of the following information associated with the loss event:

a) Initial risk event information: event information to capture a preliminary recording of the risk event such as the date of occurrence, the function in which it was discovered, the status and brief incident description, etc.

b) Reason (for occurrence): List of the cause(s) of the risk event.
c) Loss Amount (if any): Detail the cause of the loss as well as the financial impact of the loss, including a breakdown of the financial impact if available.
d) Classification (of risk event): Detailed classification of the loss as per both internal requirements specified by CNCBLB and as per Basel II requirement for regulatory calculation and reporting purposes.
e) Remedy: Provide information on the remedial action taken to resolve the issues, including resolution date, responsibility for remediation, effect on control and changes to operational procedures.
f) Recovery Information: Record information relating to the recovery of any financial losses, including the recovery type, the amount recovered, date of recovery, or if no recovery was actuated, the recovery plan proposed.

Risk Department may require additional information regarding losses and may request a detailed root cause analysis to determine preventative actions and that appropriate controls are in place to avoid event/s reoccurring.

Risk Department shall maintain a loss collection database that will capture all internal operational risk events for the analysis of potential trends that could lead to higher operational risk exposure within CNCBLB and respective mitigation plans shall be established.

Risk Event Data Analysis

Internal risk events shall be analysed by Risk Department on a periodic basis in order to identify emerging risk, control weaknesses and potentially develop risk mitigation plans. Risk Department shall make use of the data from external loss events for the purpose of periodic analysis leading to the development of mitigation plans ensuring that the external loss data corresponds and aligns well with the nature, size and lines of business in which CNCBLB operates.

Scenario Analysis

Scenario Analysis shall be used by the ManCo to identify low probability but high-impact scenarios which may result in the inability of the Group to continue operating normally.

10 Appendix C – Risk & Control Self-Assessments ("RCSA")

CNCBLB shall adopt a RCSA methodology that will support the identification of risks and establish the assessment criteria for the likelihood and impact assessment of risks and the effectiveness of the respective controls.

The following inputs and information shall be considered in order to identify risks during the RCSA process:

a) Representatives from across the full scope of the business and support function's activities;
b) Business function plan defining the objectives of the function/ process/ product;
c) Business process mapping showing key controls and highlighting recent proposed changes;
d) Key Risk Indicators;
e) Risk events databases and analysis covering both internal and external events;
f) Relevant media comments e.g. on past incidents from competitors;
g) Internal or external audit comments and recommendations; and
h) Regulator comments and recommendations.

The RCSA process shall be conducted as an interactive and cooperative effort by the function being reviewed in collaboration with the Risk Department. The frequency for conducting RCSA across the Bank shall be determined by ManCo which shall consider, among other factors, on the:

- Complexity of the process;
- Criticality of the process;
- Risk Reviews;
- Risk assessment rating assigned to the process from previous RCSA exercises; and
- Internal audit findings.

11 Appendix D – Key Risk Indicators ("KRI")

KRI Identification

CNCBLB shall adopt a methodology to establish KRIs to monitor changes in the operational risk profile, based on the strategic objectives and RCSA results.

The established KRI's shall be reviewed periodically by ARCo, at least annually, for their relevance to the Branch due to change in people, process, technology and introduction of new products.

KRI Thresholds

The business and support functions in collaboration with Risk Department shall define thresholds for identified KRI, so as to regularly assess the status of the operational risk exposure. The thresholds shall be determined taking into consideration the following criteria:

a. Risk appetite of CNCBLB as set out by the ManCo;
b. Estimation by management that shall be validated through testing over time;
c. Observed historical data (if data is available) including loss data; and
d. Benchmarking against peer banks (if data is available).

Each business and support function in CNCBLB along with Risk department shall be responsible for determining thresholds for the identified KRIs which shall be approved by ManCo.

KRI Tracking and Reporting

The risk owner shall be responsible for tracking their respective KRIs and significant breaches shall be notified to the CRO as and when they occur. The frequency of reporting KRIs shall be determined by ManCo based on the nature and type of KRI.

KRI Analysis

Risk Department shall conduct analysis of the reported KRIs in order to identify any potential trends that could lead to higher operational risk exposure within CNCBLB and appropriate mitigation plans shall be determined with the risk owners and presented to ManCo for approval.

12 Appendix E – Risk Scoring Methodology (Risk Matrix)

The 'Risk Matrix' is an internal document which is maintained by Risk Department.

This document is a consolidated view of all the identified risks within CNCBLB and is held in the secure drive n:/Risk Management/Operational Risk/Risk Matrix.

Risk Identification

Risk identification is a core component of the overarching RMF. The main features of the planned identification activities are outlined below.

The Risk Matrix

The Branch will maintain a Risk Matrix that captures all risks arising from an activity of the Branch.

With reference to the Branch's business plan, and with input from the departments and support functions, including the 2LOD functions, the CRO will conduct a full assessment of the Branch's Risk Matrix on an annual basis to ascertain its completeness. An assessment of the Risk Matrix will also be conducted whenever there is a significant change to the business, including the introduction of new businesses or new products which introduce new risks. This review is presented to the ARCo for its assessment and approval and then to the ManCo for their final approval.

The Risk Matrix includes details of the nature of the risk, the source of the risk within each business line, the owner of the risk in the 1LOD, the controls in the Risk Management Framework by which the risk is mitigated or controlled, the function in the 2LOD responsible for the relevant framework within which the risk is controlled, the committee responsible for oversight of the framework and reference to any relevant policies.

The Risk Matrix also includes an assessment of each risk in accordance with the Risk Scoring Methodology (captured in the RMF). When assessing risk, the Branch considers both the inherent (the nature of risk before any mitigants are applied) and the residual risk (the nature of the risk once respective mitigants have been applied), to ensure risks faced are within the Branch's risk appetite.

This assessment of both likelihood and impact of each risk is based on the judgement of the CRO with input from all department heads including the CCO. Any changes to the risk matrix will be reviewed and approved at least annually by the ARCo. This assessment may be informed by input from the business or support functions in which the risk arises and from historical experience.

Risk Scoring Methodology

The scoring methodology assesses:

- The likelihood of a loss event due to the risk (or control weakness); and
- The resulting impact were the event to occur.
- An overall risk score (Low, Medium or High) will be assigned to each risk by reference to the individual likelihood and impact scores.

Key risks are considered to be those inherent risk with a High overall risk score pre-mitigation that means:

- Any inherent risk with High Impact;
- Any inherent risk with a High impact and a Medium or High probability of occurring; and
- Any inherent risk with a Medium impact but a High probability of occurring.

Risk Scoring Methodology

Probability **Impact**	**Low** Event unlikely to occur in the foreseeable future: less than once in 3 years.	**Medium** Event is possible: could occur once in every 1-3 years.	**High** Event is likely to occur at least once in the next 12 months
High **Financial:** >= £500k potential or actual net profit forgone/cost incurred **Reputational:** Major damage to the Branch/Bank reputation, market value **Regulatory:** Could result in major disciplinary action by the regulator **Policies and procedures:** Non-compliance with Head Office or ManCo Approved Policies. **Business disruption:** Could result in severe business disruption **Management reporting:** Reporting to Senior Management and the President has serious deficiencies	**Medium**	**High**	**High**
Medium **Financial:** <£500k but >= £150k potential/actual net profit forgone/cost incurred **Reputational:** Significant damage to the Branch/Bank reputation, market value	**Low**	**Medium**	**High**

Regulatory: Could result in investigation/minor disciplinary regulatory action **Policies and procedures:** Non-compliance with Business Unit policies and standards **Business disruption:** Could result in serious business disruptions **Management reporting:** Reporting to Senior Management or the President has some deficiencies			
Low **Financial:** < £149k potential/actual net profit forgone/cost incurred **Reputational:** Limited damage to the Branch/Bank reputation, market value **Regulatory:** Could result in investigation/adverse comment by the regulator **Policies and procedures:** Non-compliance with Branch policies and standards **Business disruption:** Could result in some business disruption **Management reporting:** Reporting to Senior Management or the President has minor deficiencies	**Low**	**Low**	**Medium**

Probability

The probability refers to the probability of specific risk events occur without the Branch taking any actions under the current level of assets, business environment, market competition or market conditions. The Branch has classified the probability of risk into three categories. A table illustrating this can be found below:

Probability Risk Scoring Criteria

Criteria	Probability
Unlikely: Event is unlikely to occur in the foreseeable future (less than once every 3 years).	Low
Possible: Event could possibly occur (once in every 1-3 years).	Medium
Likely: Event is likely to occur (at least once in the next 12 months).	High

Severity

The severity of risk specifically refers to risk events that have occurred, resulting in either a direct or an indirect loss for the Branch. When classifying the severity of risk, the Branch first assesses whether the risk has a financial or a non-financial impact. Definitions of these terms can be found in the table below.

Definitions of Impact

Impact type	Definition
Financial impact	Financial impact assesses once the risk events occurs whether will lead to major financial impact or loss.
Non-financial impact	Non-financial impact assesses once the risk events occur, the impact on Branch's reputation, external institution's (regulator, rating agency) reaction as well as the impact on other business departments.

Once it has been established whether the risk event that has occurred has had either a financial or a non-financial implication for the Branch, the severity of the risk will then be considered. In order to measure this the Branch will use specific criteria which is mapped against the Bank's profit from the previous year. The table below outlines the severity levels used by the Branch and their subsequent criteria.

Severity Level Criteria

Severity	Criteria
High	**Financial:** >= £500k potential or actual net profit forgone/cost incurred **Reputational:** Major damage to the Branch/Bank reputation and/or market value **Regulatory:** Could result in major disciplinary action by the regulator **Policies and procedures:** Non-compliance with Head Office or ManCo Approved Policies. **Business disruption:** Could result in severe business disruption
Medium	**Financial:** >£499k but < £150k potential/actual net profit forgone/cost incurred **Reputational:** Significant damage to the Branch/Bank reputation and/or market value **Regulatory:** Could result in investigation/minor disciplinary regulatory action **Policies and procedures:** Non-compliance with policies and standards **Business disruption:** Could result in some business disruption
Low	**Financial:** < £149k potential/actual net profit forgone/cost incurred **Reputational:** Limited damage to the Branch/Bank reputation and/or market value **Regulatory:** Could result in investigation/adverse comment by the regulator **Policies and procedures:** Non-compliance with policies and standards **Business disruption:** Could result in minor business disruption